#4
DB
7-31-01

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	Martin EUCHNER
ATTORNEY DOCKET NO.:	P01,0142
INTERNATIONAL APPLICATION NO:	PCT/DE99/03262
INTERNATIONAL FILING DATE:	11 OCTOBER 1999
INVENTION:	METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

Assistant Commissioner for Patents,
Washington D.C. 20231

INFORMATION DISCLOSURE STATEMENT
According to 37 C.F.R. 1.97(b)

Sir:

In accordance with the provisions of 37 C.F.R. 1.56 and the requirements of 37 C.F.R. 1.98, Applicant respectfully requests that a citation and examination of the references identified on the attached PTO 1449 form be made during the course of examination of the above-identified application for United States Patent.

The present Information Disclosure Statement is being filed according to 37 C.F.R. 1.97(b) and before the latter occurrence of:

(1) three months from the filing date of a national application;

(2) three months from the date of entry of the national stage as set forth in 37 C.F.R. 1.491 in an international application; or

(3) the mailing date of a first Office Action on the merits.

REMARKS

The attached PTO 1449 form lists related art references for the above identified application, including those identified in the International Search Report, copy of which is enclosed herewith.

EXPLANATION OF RELEVANCE

References AA, AJ, and AN-AP were cited in the International Search Report. References AQ-AV were cited in the Specification. All references are in English and thus require no further commentary, except references AQ-AR (whose relevance is adequately discussed in the Specification) and reference AJ, which is a German Patent. An English language translation of the abstract for AJ is provided, and a complete translation of the reference will be produced for the Examiner upon request.

The filing of the present Information Disclosure Statement is not to be construed as a representation that a search has been made, and is not to be construed as an admission that the information cited in the present Information Disclosure Statement is, or is considered to be, material to patentability as defined in 37 C.F.R. 1.56(b).

The above citation of related art is not a representation that such art constitutes a complete or exhaustive listing of all pertinent related art, nor that it necessarily includes the closest or most relevant art. The aforementioned citation comprises a voluntary citation of related art of which applicant and his attorney are presently aware and is not intended to serve as a substitute for the Examiners own search.

Submitted by,

Mark Bergner (Reg. No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
Chicago, Illinois 60606-6473
(312) 258-5779
Attorney for Applicant(s)

CUSTOMER NUMBER 26574

Form P.T.O. 1449U.S. Department of Commerce Patent and Trademark Office LIST OF RELATED ART CITED BY APPLICANT (use several sheets if necessary)	Docket No.: **P01,0142**	Serial No. **New Application**
	Applicant(s): **Martin EUCHNER**	
	Filing Date **Herewith**	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner's Initials		Document Number	Date	Name	Class	Subclass	Filing Date If appropriate
	AA	5,241,599	August 31, 1993	Bellovin et al			
	AB						
	AC						
	AD						
	AE						
	AF						
	AC						
	AH						
	AI						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Subclass	Translation	
							Yes	No
	AJ	DE 39 15 262 A1	30 November 1989	Germany				
	AK							
	AL							
	AM							

OTHER RELATED ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AN	HARN, L, "Modified key agreement protocol based on the digital signature standard", Electronics Letters, (1995) UK, Vol. 31, No. 6, pp. 448-449.
	AO	DIFFIE W, et al, "Authentication and authenticated key exchanges", DESIGNS, CODES AND CRYPTOGRAPHY, (1992), Netherlands, Vol. 2, No. 2, pp. 107-125.
	AP	KOBLITZ, N. , "Elliptic curve cryptosystems" Mathematics of Computation, (1987), USA, Vol. 48, No. 177, pp. 203-209.
	AQ	RULAND, C., "Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim (1993), ISBN 3-89238-081-3, pp. 42-46.
	AR	RULAND, C., "Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim (1993), ISBN 3-89238-081-3, pp. 73-85.
	AS	RULAND, C., "Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim (1993), ISBN 3-89238-081-3, pp. 101-117
	AT	NIST, FIPS PUB 180-1: Secure Hash Standard, (1995), http://csrc.nist.gov/fips/fip180-1.ps
	AU	NIST, FIPS PUB 81: DES Modes of Operation, (1980), http://ww.itl.nist.gov/div897/pubs/fip81.htm
	AV	MENEZES, A. et al., Handbook of Applied Cryptography; CRC Press (1996), ISBN 0-8493-8523-7; chapter 12.6, pp. 515-524

Examiner	Date Considered

***EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.**